



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 7 Number 2, February 2004

From the case files of

The LUBRINCO Group

<http://www.lubrinco.com/>

and

Financial Examinations and Evaluations, Inc.

<http://www.feeinc.com/>

Concealed assets in fraud, theft, and divorce? Call us!

This month's features:

- 1. Due Diligence — Small frauds**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Why we manage vulnerability, not risk or threat**
- 3. Executive Protection — Stop before you enter**
- 4. Technical Issues — A new credit card scam**
- 5. Real Stories from the Field — Stupid training tricks: Get out your checkbook**
- 6. Book and Product Reviews — Motorola V-600 quad-band handset**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Small frauds

We recently got an inquiry about someone who had invested \$17,000 of her own money, and \$23,000 of other people's money, in a deal allegedly to develop computer-based training for schools in Africa, first in Zimbabwe, then working up to Cairo. The project was said to be coordinated through the Bank of Ghana, which had received a \$55 million dollar grant to buy equipment and put the program in place. The investor would be the owner of the company, according to the promoters and 70% of it would be profit.

With \$55 million in play, why was her money needed? Well, they needed cash for the insurance (\$10,000), and money for what was termed "blessings," which certainly sounds better than bribes, which are illegal. Since the return on investment was so high, it seemed worth the investment to the poor victim.

The details of the fraud are not terribly important, since it looks a great deal like most frauds of this kind. There was an appeal to greed, a good deal of stroking involved, a lot of faxing of official-looking documents, a lot of international calls to seemingly-important people, no verification (by the victim) of anything that was going on, and a concerted effort to overlook the question of whether the deal made any sense.

Did she ask for outside advice on the deal? Certainly: She is, after all, a teacher, and no fool! Her lawyer, and, apparently everyone else with whom she consulted, said she should absolutely *not* do this. But the deal was so good, who could resist?

Now, stripped of her life's savings, possibly obligated personally for the monies given directly to her by the other investors, and negotiating with her telephone company about paying for the many thousand dollars of calls to Africa – ostensibly to the direct line of the President of the Bank of Ghana – she is still convinced that the deal will go through, and will likely borrow more money to cover unexpected costs that have delayed her money being sent to her.

In another case, less egregious only because it did not wipe the victim out, an investment banker mentioned that a friend of theirs had invested in a high-yield scheme without bothering to ask for advice. Since the current WSJ Prime Rate is 4.000, the Federal Discount Rate is 2.000, the Fed Funds Rate is 1.000, and the 11th District Cost of Funds is 1.821, it shouldn't take a rocket scientist to guess that a guaranteed return of even 20% APR should make you more than a trifle suspicious.

For fraud to be successful there generally need to be two willing participants, one of whom is the victim. As W. C. Fields noted, you can't cheat an honest man, so there has to be a sufficient level of greed to overcome common sense and, sometimes, moral standards. As always, if it sounds too good to be true, it almost certainly isn't true, and you are likely to lose everything you invest.

Most of our readers, we hope, will have little contact with fraudsters. Yet a lot of people are getting defrauded on a regular basis in scams that look, to the outsider, like, well, scams.

On one end of the spectrum you have the obvious scam by e-mail asking for you to act as the conduit for funds hidden away by the writer's now dead relative who had a position of power in his African government. On the other end, are the very accomplished fraudsters who are repeatedly able to "sell" shares in companies, future profits in new technologies, and a range of other products for which the wealthy or not-so-wealthy would-be investor hands over substantial sums of money to an individual or sham company. Tragically, most are later so embarrassed at having been taken that the fraudster is rarely brought to justice.

If you want to see how good some of these people are, just answer one of the many scam e-mails you get every day. The correspondence will provide you with endless amusement, but DON'T send money, DON'T send account information, DON'T send personal information, and DON'T make expensive international calls.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Why we manage vulnerability, not risk or threat

Someone asked us the other day why we say we manage vulnerability, not risk. Why are we vulnerability managers, not risk managers? In order to understand this, it is important to refresh your memory about the fact that risk is *derived* as the product of other factor. It is not itself an underlying characteristic that can be controlled.

Risk is calculated as:

$$\mathbf{Risk = probability \times impact}$$

Where:

$$\mathbf{Probability = threat \times vulnerability}$$

So that risk becomes:

Risk = threat × vulnerability × impact

Now, we cannot generally control a threat. That is to say, we do not, either as individuals or corporations, have a whole lot of control over whether someone wants our information. We know that most of us work for companies that have competitive intelligence departments because our companies want information on our competitors. And we know that they have competitive intelligence departments, too, and that there isn't any reason to assume that their staff is significantly less competent than is ours. We also know that foreign competitors, and sometimes even foreign governments, want our information. Even worse, we know that some of these adversaries willingly commit illegal acts to get what they want. There is not a lot we can do to reduce this threat.

In terms of impact we are equally powerless: It is what it is. If a competitor takes our marketing plans or the production figures for our top sales people or our trade secrets, there will be an impact. We will be able to assess the damage, but the result of the assessment is pretty much out of our control.

This leaves vulnerability, in which we do have some control in three areas. We can manage it, we can transfer the vulnerability, and we can accept it.

Managing vulnerability

Managing vulnerabilities means we can find ways to identify and reduce the vulnerabilities. In the case of information, we can try to make it more difficult to steal. As an example, if you are a U.S. citizen you probably wouldn't want your tax returns made public. Neither would Uncle Sam. So the people in India who process your returns are not allowed to bring in cameras or notebooks, or, hopefully, anything else that would allow your information to be copied.

If you have trade secrets, you might put them on particularly eye-catching paper, lock them in a special place, require two trusted staff members to get access to them, have a room next to where they are stored that is the only place they can be seen.

You might figure out which of your adversaries is willing to go the extra mile to get your information, what exactly they need, how (or through whom) they are planning to get the information they need, and put in countermeasures to reduce the likelihood of their success.

Transferring vulnerability

Through insurance, you can transfer the cost of damages caused by adversaries and competitors exploiting your vulnerabilities. If you suffer a loss of information, some of your loss is repaid.

Accepting vulnerability

You may decide, either deliberately or because you haven't thought about it, that your vulnerability is sufficiently low that the ensuing risk doesn't bother you, and take no defensive actions.

But here's the rub: Accepting the risk that is attached to your vulnerability is generally a decision that is not actually made. Rather, it is often something that simply happens because nobody has given it any thought. Thus, even companies that have established competitive intelligence departments are unlikely to have anyone responsible for combating espionage, and therefore nobody is responsible for the identification of vulnerabilities – the only piece of the puzzle that can be managed.

So when you bring us in to help you assess your risk, what you are really looking for is help in determining the threats against you, determining the impact if these threats are fulfilled, and managing your vulnerabilities to help minimize your risk.

3. Executive Protection — Stop before you enter

Last year someone behind us practically knocked this writer over when we stopped before entering a store. They asked why we had stopped, and we said that we wanted to make sure there was nothing bad happening in the store before we went in. They muttered something unintelligible, out of which we think we heard the words “paranoid” and “fruitcake.”

We were reminded of this earlier this week when we got a call from a friend saying that someone we had met had gone into a bank where there was a robbery in progress, and was, sadly, killed.

Now, it is certainly true that you are probably no more likely to be struck by lightning than you are to walk into a crime in progress and end up dead. Nonetheless, rare as a lightning strike may be, the prudent person does not walk across the fairway during a thunderstorm while holding a nine-iron above their head. At least not a second time....

It is equally true that you are very unlikely to walk in on a crime. But, just as people do get struck by lightning, people do walk into crimes in process.

While there is sometimes no warning and no way it could be prevented, in many cases there is. Please understand that we are not talking about crimes aimed at you, which should have been spotted in advance. We are talking about a chance encounter, where often there is a warning.

Before we enter a business establishment we look through the window to see if there is something amiss, and then, when we open the door, we look again, giving us a final option to push back to safety. What are we looking for? Well, the primary thing we want to see is normal movement. If people are moving around, chatting, picking things up, and even walking out of the store. If people are frozen in place, this is a very bad sign. If they are frozen in place and there are one or more people with guns, it is a worse sign, and you should push backward out of the doorway and get away fast. Then call the police.

In some cases there are other clues. We once came home and discovered that the door to our apartment was unlocked. Now, there are many possible reasons why this could happen, but none of them justified our going into an apartment whose door should have been locked. Instead, we went downstairs to the street, flagged down a passing police car, and asked them to go in and look. They found nothing, and it later turned out that someone (else) had left the door unlocked, so that anybody could have gone in. Did we feel silly at having the cops go in? Not at all.

There are a large number of things we can do to stay safe that do not involve a lot of cost or effort. Merely wearing your seatbelt and giving up smoking will do a lot to prolong your life. And adding to the basics other painless things like looking into store before you go in takes mere seconds, and could save your life.

4. Technical Issues — A new credit card scam

The following came to us through InfraGard via the Atlanta chapter of ASIS. Since it is a relatively new and sophisticated scam, we thought it was worth reprinting here:

We all receive emails all the time regarding one scam or another; but last week I REALLY DID get scammed! Both VISA and MasterCard told me that this scam is currently being worked throughout the Midwest, with some variance as to the product or amount, and if you are called, just hang up.

My husband was called on Wednesday from “VISA” and I was called on Thursday from “MasterCard”. It worked like this: Person calling says,

“This is Carl Patterson and I'm calling from the Security and Fraud department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card issued by 5/3 bank. Did you purchase an Anti-Telemarketing Device for \$497.99 from a marketing company based in Arizona?”

When you say “No,” the caller continues with, “Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from \$297 to \$497, just under the \$500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?” You say, “Yes”.

The caller continues, “I will be starting a fraud investigation. If you have any questions, you should call the 800 number listed on your card 1-800-VISA and ask for Security. You will need to refer to this Control #”. Then gives you a 6 digit number. “Do you need me to read it again?” Caller then says he “needs to verify you are in possession of your card. Turn the card over. There are 7 numbers; first 4 are 1234(whatever) the next 3 are the security numbers that verify you are in possession of the card. These are the numbers you use to make internet purchases to prove you have the card. Read me the 3 numbers.” Then he says, “That is correct. I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions? Don't hesitate to call back if you do.”

We actually say very little, and they never ask for or tell you the card number. But after we were called on Wednesday, we called back within 20 minutes to ask a question. Are we glad we did! The REAL VISA security dept. told us it was a scam and in the last 15 minutes a new purchase of \$497.99 WAS put on our card.

Long story made short, we made a real fraud report and closed the VISA card, and they are reissuing us a new number. What the scam wants is the 3 digit number! Once the charge goes through, they keep charging every few days. By the time you get your statement, you think the credit is coming, and then it's harder to actually file a fraud report.

The real VISA reinforced that they will never ask for anything on the card (they already know). What makes this more remarkable is that on Thursday I got a call from “Jason Richardson of MasterCard” with a word for word repeat of the VISA Scam. This time I didn't let him finish. I hung up. We filed a police report (as instructed by VISA), and they said

they are taking several of these reports daily and to tell friends, relatives, and co-workers.

5. Real Stories from the Field — Stupid training tricks: Get out your checkbook

Those of you who read *ÆGIS* regularly know that we are big believers in training. More than that, we are big believers in realistic, scenario-based training. However, while we believe training should be as realistic as possible, we don't believe that it should be a surprise. That is to say, every participant should know that the training is training, not real life.

We also need to take every safety precaution. Thus, when we train police officers, we make sure that there are no functioning weapons available to them: No functioning firearms, no knives, and no impact weapons. This way we don't have to worry about someone accidentally hurting someone, or getting so carried away by the scenario that they do something harmful.

This approach is not unique to us, of course, and is, in fact, the general approach taken by most trainers.

We were therefore distressed to read an article by David Hendee in the 9 December 2003 issue of the *Omaha World-Herald* about a training exercise jointly performed by the Lincoln-based *Gas 'N Shop* convenience stores and the Schuyler Police Department. According to the description given in the article by one of the victims, Kristin Johnson:

"We were just chit-chatting, waiting for a manager who was late, and these two guys come running into the store. One yelled, 'Get down on the floor! Get down on the floor!' He had a shotgun. . . .

"I immediately hit the floor. He started yelling for our purses."

According to the article, "Johnson said she couldn't bring herself to go to work the following Monday because of anxiety. She worked a few hours Tuesday and quit." We don't know whether she merely left early, or quit for good after being thus traumatized.

Assuming the report was accurate, *Gas 'N Shop Inc.* and the Schuyler Police Department were very fortunate that there were no armed employees, civilians, or off-duty officers unwittingly on the scene, that no employees decided to fight back, and that no employees with weak hearts died, any of which would have turned an exercise of bad-judgment into a needless tragedy.

In the future, employees may well assume that any bad thing that actually happens is a drill, and do something foolish. The company will certainly

have to deal with employees who quit, or suffer some sort of temporary or even permanent physical or psychological damage

We have not followed up on this, but if the World-Herald report is true, both Gas 'N Shop Inc. and the Schuyler Police Department face a very strong negligent action suit: They knew, or should have known, that what they did was a dangerous practice. We have discussed this case with a number of prominent law enforcement trainers, all of whom would be delighted to testify for the plaintiff in a case this egregious.

We certainly hope any company or police department that would pull a stunt like this would also do role-playing on writing settlement checks.

6. Book and Product Reviews

Motorola V600 quad-band handset

http://commerce.motorola.com/consumer/QWhtml/m_v600.html

Motorola is the second company, after NEC (see the August 2003 e-journal), to venture into the world of quad-band GSM devices, with three current offerings, the V400, V500, and V600. We are looking here at the V600.

The primary virtue of the V600 is that it is a quad-band GSM device, with what appears to be a very good radio. If you do not travel outside of North America you can stop reading here, since a quad-band device only makes sense for an international traveler: You would be better served with an 850/1900 MHz dual-band GSM handset for use in North America.

Where do you need which frequencies? In general you need 900 MHz and 1800 MHz to get widest GSM coverage outside the Americas. You need 850 MHz and 1900 MHz to get widest GSM coverage in North America now that Cingular and AT&T Wireless have implemented GSM 850. You need all four bands to get complete GSM coverage in Latin America and the Caribbean, where some areas have implemented one *or more* frequencies from **both** the 850/1900 MHz frequency pair *and* the 900/1800 MHz frequency pair. If you travel frequently between the Americas and any of the other places having GSM coverage, the V600 could be a good choice.

In terms of the handset itself, the screen is **very** readable, and the ring tones are the loudest we have heard. As mentioned, the RF portion of the V600 is excellent, and the battery is actually better than most that Motorola has offered. The 750 mAh battery is rated to give you between 3.5 and 7 hours talk time, depending on what power level it is using internally. This means if you want to be able to talk through a blackout you need to plan on carrying

at least a second battery with you, which, by today's standards is considered to be quite acceptable.

The V600 has Bluetooth, so you will be able to use a wireless earpiece/microphone and car kit, thus sparing you the inconvenience of wires. It is GPRS enabled, but is not EDGE enabled. This is not a big deal, because data in handsets is currently limited by SAR rating (which at the ear is 1.09 W/kg (we prefer it to be under 0.5), and on the body is 0.25 W/kg. The SAR value for this product in its data transmission mode (body-worn use) is 0.50 W/kg). If you want a wireless connection to your laptop you will be better off with the data speed available with current 4/2 timeslot EDGE technology in a PCMCIA card, without worrying about emission levels.

For those who want easy access to the features of the handset, the V600 should work well with Motorola's Mobile PhoneTools, allowing you to connect it to your laptop to enter phone numbers, send and receive text messages, and use the calendar function.

The bottom line is that GSM 850 has now become a necessity, and if you travel from North America to GSM 900/1800 areas you need all four bands.

Nokia, which does not make a quad-band terminal, says:

“Assuming that a traveler who has occasion to visit markets in which they need each of the 4 possible GSM bands, there are really 2 basic solutions.

1) If the user prefers to carry one device, then a quad mode phone may be the best possible option.

2) If the user would rather be able to choose from the much larger universe of tri-mode phones, he could choose to buy a GSM 850/1900/1800 handset along with a GSM 900/1800/1900 handset. For consistency, he would probably want to buy the same basic handset, just in different flavors so as to not need to learn 2 UIs, use common accessories and to facilitate backing up the information between handsets.”

The bad news is that, unlike the NEC 515, the V-600 includes a camera, which immediately disqualifies it for the business user. This is because there are an increasing number of schools, businesses, health clubs, retail clothing stores, restaurants, and facilities where camera phones are banned. In some cases they are confiscated, and in others they are destroyed, and we understand that some businesses will summarily fire any employee found with a camera phone. For the traveler for whom the camera is not an immediate disqualifier, who travel extensively, and who don't wish to carry two dual- or tri-band handsets, the V600 is worth serious consideration.

7. Free-Subscription/Unsubscription/Copyright Information

•• ÆGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2004 by The LUBRINCO Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@lubrinco.com).

The LUBRINCO Group provides services in three high-threat areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

- **Protection of trade secrets and intellectual assets.**
 - Anti-economic espionage.
 - OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.
- **International financial investigations and due diligence consulting.**
 - Location and recovery of missing and hidden assets.
 - Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
 - Anti-money laundering and financial fraud requirements under the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2004* and the *EU Revised Money Laundering Directive of 2004*.
- **Protection of management, staff, and families.**
 - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
 - When traveling and living overseas.
 - When transporting items of substantial value.

LUBRINCO identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff.

For information on **The LUBRINCO Group** and its services, or for the archive of all past issues of ÆGIS e-journal in PDF format, please go to <http://www.lubrinco.com/>.

To sign up for a **complimentary subscription** to ÆGIS e-journal or the ÆGIS e-journal PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to ejournal@lubrinco.com.

To subscribe to our AvantGo channel, go to http://avantgo.com/channels/_add_channel.pl?cha_id=1773

To be removed from the subscription list, follow the instructions on the mailing you received, or send an e-mail to ejournal@lubrinco.com.

If you know of anyone else who should be receiving ÆGIS e-journal, please send their e-mail address to ejournal@lubrinco.com.

If there is a topic that you would like to know more about, send it to ejournal@lubrinco.com and the editors will consider it as the topic for an article in an upcoming issue.

If you would like to submit an article for publication in ÆGIS e-journal, send it as an attachment to an e-mail to ejournal@lubrinco.com. Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in ÆGIS e-journal constitutes a license to The LUBRINCO Group Ltd, Inc., and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

If you would like to go beyond normal fair-use in reproducing articles from this issue of ÆGIS e-journal, you may do so freely as long as appropriate source, copyright, accreditation, and link to the LUBRINCO website is included. This should be in the form

Article Title, from the February 2004 ÆGIS e-journal (© 2004 LUBRINCO & FEE), to be found at <http://www.lubrinco.com/>.

ÆGIS e-journal is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in ÆGIS e-journal should be

construed as legal advice. The information provided is “general information,” not “specific advice.”

The solution to any problem is highly dependent upon the precise facts involved. Thus, before making any reliance upon anything said here, you should consult with an appropriately skilled professional. Opinions expressed by contributors are not necessarily endorsed by the publisher, and may be presented to encourage a dialogue among subscribers. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in *ÆGIS* e-journal.

Please be safe, and be smart.